FACT SHEET

U.S. Army Cyber Command

The Nation's Army in Cyberspace

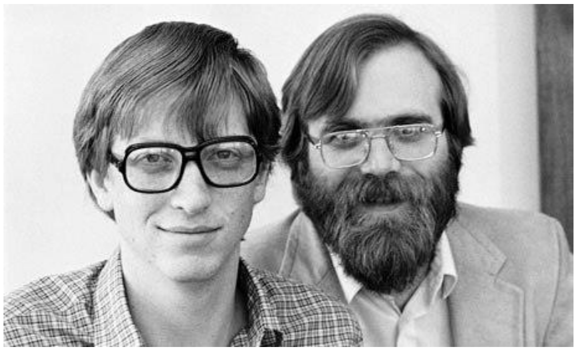
www.arcyber.army.mil • www.army.mil/armycyber • @ARCYBER

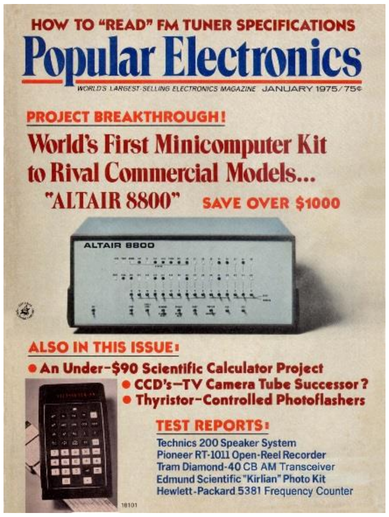
THE FACTS: THE HISTORY OF COMPUTER HACKING

When commercial computers were first developed, people assumed it to be a benign environment, but computer crime evolved with computer development. Beginning in the early 1950s, unscrupulous insiders successfully began using computers for fraud and embezzlement.

The first concerns about computer vulnerability emerged in the 1960s. The spread of personal computers, beginning in the late 1970s, coupled with the development of the Internet in the late 1960s and the World Wide Web in 1991, further fostered the spread of abusers – hackers -- who sought to gain unauthorized access to computer systems.

In December 1974 Micro Instrumentation and Telemetry Systems (MITS) introduced a mail-order, build-it-yourself 256-byte computer kit called the Altair 8800 and started the personal computer revolution. Its output was displayed by a bank of lights and users had to input data by flipping toggle switches. Thousands of people bought the $400 kit, making it the first commercially successful home computer. Its success led to the first retail computer store in 1975 and the first computer clubs nationwide.

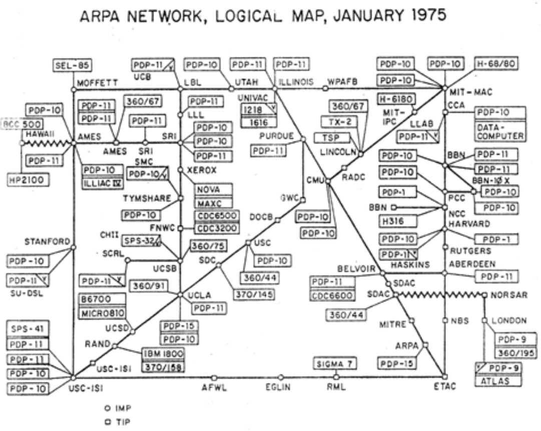



HOW TO "READ" FM TUNER SPECIFICATIONS
Popular Electronics
WORLD'S LARGEST-SELLING ELECTRONICS MAGAZINE JANUARY 1975/75¢
PROJECT BREAKTHROUGH!
World's First Minicomputer Kit to Rival Commercial Models...
"ALTAIR 8800"
SAVE OVER $1000
ALTAIR 8800
ALSO IN THIS ISSUE:
• An Under-$90 Scientific Calculator Project
• CCD's–TV Camera Tube Successor?
• Thyristor-Controlled Photoflashers
TEST REPORTS:
Technics 200 Speaker System
Pioneer RT-1011 Open-Reel Recorder
Tram Diamond-40 CB AM Transceiver
Edmund Scientific "Kirlian" Photo Kit
Hewlett-Packard 5381 Frequency Counter
10101

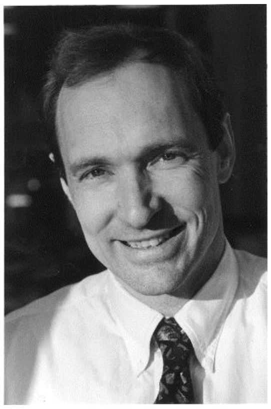
After reading about the Altair in the January 1975 issue of *Popular Electronics,* Paul G. Allen (right), a computer programmer for Honeywell in Boston, and his boyhood friend Harvard sophomore William H. Gates III (left) were hired by MITS to adapt the Beginners All Purpose Symbolic Code (BASIC) programming language for the Altair. Allen and Gates took the money they made from "Altair BASIC" and formed their own company that year. It was called Microsoft, for "microcomputer software."

In 1976 Steve Wozniak (left) and Steve Jobs (right), engineers in a California computer club, built a homemade computer called the Apple I (top). More sophisticated than the Altair, it could be hooked up to a color television and store data on an external cassette tape. They sold 200 units at $666 each. A year later they introduced the more refined Apple II (bottom) that sold for $1,300. The Apple II's programs made it a practical tool for all kinds of people and businesses, and it soon became a leader in the growing personal computer market.

By 1978 personal computers were turning America into a computerized society. In February, two Chicago PC users reportedly established the nation's first electronic bulletin board, allowing multiple users to share information. The conceptual precursor to today's Internet web page, bulletin boards spread widely and were operated by disparate groups and individuals. Anyone with a PC could set up an electronic bulletin board.

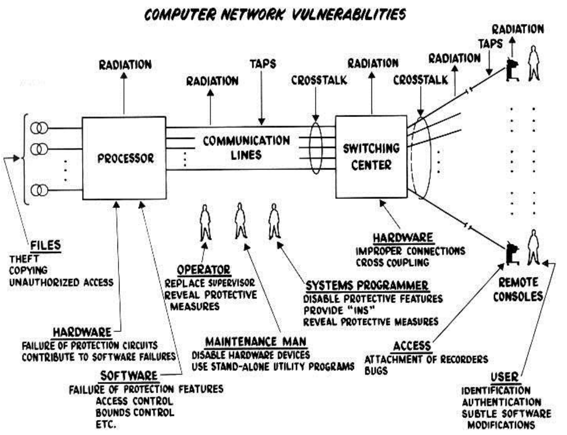


In 1969 the DoD Advanced Research Projects Agency, ARPA, had demonstrated the practicality of an interconnected computer network that initially allowed university researchers doing ARPA research to communicate with each other. It later expanded to include government, industry and major universities in the U.S. and Europe. The number of networks grew in the 1970s and increased significantly as the personal computer revolution spread. For example, there were 61 ARPANET computers in 1975, nearly 30,000 by the end of 1987 -- when ARPANET became known as the Internet -- and more than 160,000 by the end of 1989.



In 1989 Timothy Berners-Lee, an English computer scientist working at the European Council for Nuclear Research (left), successfully implemented the use of hypertext to facilitate sharing and updating information on the Internet, earning him the distinction of inventing the World Wide Web. The European Council for Nuclear Research built the first website, which went online August 6, 1991.

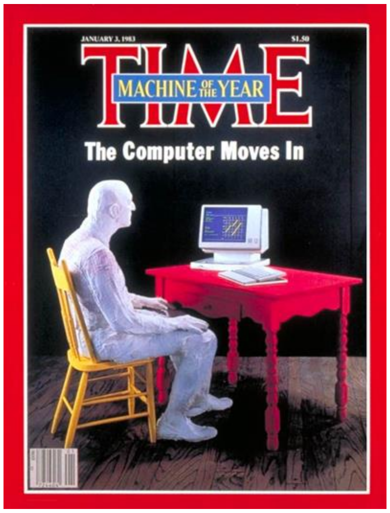
The Defense Department had already became concerned with computer security in 1967 as resource-sharing computer systems spread in the DoD. The Defense Science Board assembled a task force that year to study classified



computer security safeguards. Their report, issued in 1970, showed how corrupt insiders and spies could actively penetrate computers and steal or copy classified information. The study led to more than a decade of activity by government hackers who tried to break into sensitive computers and succeeded in every attempt. DoD established uniform policies for protecting classified computer systems in 1972 and 1973.

The term "hacker" reportedly originated at the Massachusetts Institute of Technology in the 1960s, where it initially meant someone who knew everything there was to know about computers. By the early 1980s the term evolved to describe anyone who could invade someone else's computer. In 1983 this new breed of hackers began receiving widespread attention. First, the film "Wargames," released in June, told the fictional tale of a high school hacker who breaks into the North American Air Defense Command computer system to run a nuclear war simulation he thinks is a computer game, nearly starting World War III. The film inspired a group of Milwaukee teenagers, known as the "414s" after their telephone area code, to break into dozens of computer systems nationwide, including an unclassified government computer at the Los Alamos National Laboratory, a nuclear weapons facility in New Mexico. In the fall, CBS TV aired "Whiz Kids," a show that glorified four high schoolers who used their hacking skills to help solve crimes.

The DoD first became concerned about possible Soviet hacking into its systems after the Los Alamos incident and hackers breached the ARPANET trying to access classified intelligence information, as well as trying to break into Pentagon and CIA computer systems.



By the end of 1983 it became clear that personal computers created opportunities for unprecedented widespread hacker abuse. In September the *New York Times* reported:

"The number of young people roaming without authorization through some of the nation's most sophisticated computer systems runs into the hundreds and possibly thousands, according to computer crime experts. Further, they say, the number is growing hand-in-hand with the boom in personal computers.

"These electronic explorations are no longer the province of a few highly skilled computer science experts. The relatively low cost of computer equipment and the existence of electronic bulletin boards that permit the fast, nationwide exchange of information have opened

up the pathways to a vast universe of curious young people who often have only a rudimentary knowledge of the field."

In October 1983 the FBI launched a nationwide crackdown on the homes of 19 young hackers in an investigation of unauthorized intrusions into dozens of large commercial and DoD computers. No arrests were made, since there were no federal laws at that time against unauthorized intrusion into computers. That came later, in 1986.

A month after the FBI raids Fred Cohen, a University of Southern California graduate student (top photo), developed the first computer virus in a controlled experiment. Within a few years malicious hackers, mostly disgruntled employees at first, began creating serious problems by spreading viruses to sabotage their company or organization computer systems.

In September 1988, Donald Gene Burleson, a former programmer at a Fort Worth, Texas, insurance and brokerage firm (at far left), was the first person to be convicted for spreading a computer virus. Two days after he was fired in 1985, he had planted a virus in his former employer's system that wiped out 168,000 records.

In November 1988, Robert T. Morris Jr., a Cornell University computer science graduate student (left), unleashed the first large-scale malware attack on computer systems and raised public awareness about the vulnerability of computers and the Internet to such attacks. It was a malevolent computer "worm," a self-replicating program that did not destroy data, but temporarily disabled about 10 percent of the Internet, or about 6,000 computers at that time. Morris' goal was benign, to estimate the size of the Internet, but a design error in his program caused it to replicate out of control.

In July 1989 the Government Accountability Office issued a computer security report that highlighted the vulnerability of the nation's computer networks to a virus attack. The following year, the DoD and the private sector experienced widespread network vulnerability when a Bulgarian worldwide virus called "Dark Avenger" infected many of the DoD's 400,000 personal computers.

The U.S. Army first looked at developing an offensive cyber capability using viruses in 1990, when the Center for Signals Warfare at Vint Hill Farms Station, Va., sought to develop malicious software concepts to use against an adversary. The challenge was how to get the virus into an adversary's command and control systems.

In 1994 the DoD examined the vulnerability of its networks to hackers. That year Defense Information Systems Agency (DISA) hackers made about 12,000 attempts to gain entry into DoD computers. They were successful 88 percent of the time, and 96 percent of the time their intrusions were undetected. That year there were 255 known hacker attacks against DoD networks, but in reality there were several hundred thousand, and the intrusions were increasing rapidly each year.

In June 1997 the DoD conducted its first large-scale test of its ability to work with other government branches to respond to a cyber attack on the national information infrastructure. In Exercise ELIGIBLE RECEIVER, teams from the National Security Agency equipped with off-the-shelf computers demonstrated they could disrupt computer operations at major military commands and interrupt electrical power and emergency phone service in several U.S. cities. The exercise revealed that the DoD and government were unprepared to respond to such cyber attacks.

In February 1998 the Pentagon suffered the most organized and systematic attack on its unclassified computer systems to date. Over the course of three and a half weeks, a group of American and Israeli teenage hackers broke into 11 DoD computer systems. Initially believing this might be a state-sponsored attack, DoD leaders took the unprecedented step of mobilizing a special crisis cell on the Joint Staff under Operation SOLAR SUNRISE to deal with the intrusions.

In March 1998, Operation MOONLIGHT MAZE, a joint law enforcement, military and government effort, began responding to a massive attack on U.S. computer networks associated with defense and national security that was traced to unknown hackers in Russia. The attacks persisted for years, causing one of the most potentially damaging breaches of DoD computer systems and reportedly triggering the largest cyber-intelligence investigation to date.

In the wake of cyber vulnerabilities revealed by Exercise ELIGIBLE RECEIVER and Operation SOLAR SUNRISE, DoD created Joint Task Force-Computer Network Defense (JTF-CND) under U.S. Space Command in December 1998 to serve as a focal point to defend DoD computer networks. JTF-CND was co-located with DISA in Arlington, Va. With added missions, including offensive cyber operations, the organization became the JTF-Computer Network Operations (JTF-CNO) in April 2001 and, in October 2002, with the disestablishment of U.S. Space Command, the JTF-CNO was realigned under U.S. Strategic Command.

In March 1999, during the NATO air campaign over Kosovo, the DoD launched limited cyber attacks against Serbian computer networks. Later that year the U.S. intelligence community mounted cyber attacks on foreign bank accounts of Yugoslav President Slobodan Milosevic (left) and other Serbian leaders to drain their assets or alter their bank records.

China, outraged over the May 7, 1999, bombing of the Chinese embassy in Belgrade by NATO, resorted to a series of cyber attacks against the United States. Chinese hackers attacked websites of the Department of Energy, the Department of the Interior, the National Park Service and took down the White House website for three days.

In October 1999, DoD conducted a second cyber exercise called ZENITH STAR to test the lessons learned from ELIGIBLE RECEIVER. National Security Agency hackers attacked power systems feeding several U.S.

military bases and overwhelmed local 911 emergency systems with a flood of computer-generated calls. The test showed some improvement had occurred since ELIGIBLE RECEIVER, but coordination between government agencies was still poor and the national infrastructure remained vulnerable to attack.

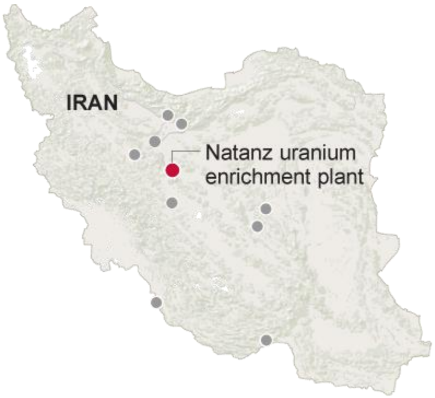
In July 2002 President George W. Bush signed National Security Presidential Directive 16, To Develop Guidelines for Offensive Cyber-Warfare, for determining when and how the United States would launch cyber attacks against adversary computer networks.

In 2005 China's army emphasized hacking as an offensive weapon during its military exercises, including hacking "primarily in first strikes against enemy networks."

On August 5, 2008, the first major cyberattack on a nation's infrastructure occurred when the Baku-Tblisi-Cuyhan oil pipeline in eastern Turkey exploded. Hackers on site, believed to be Russian or Russian-backed, infiltrated pipeline surveillance systems and valve stations and super-pressurized oil in the pipeline, causing the explosion. The Kurdistan Worker's Party, a pro-Kurdish organization with ties to Russia, claimed credit for the attack, which occurred two days before the Russian invasion of Georgia. The August 7-12 armed conflict between Georgia, the Russian Federation, and the Russian-backed breakaway republics of South Ossetia and Abkhazia, saw Russian and Georgian hackers launching a series of cyber attacks against each other. The attacks disrupted a number of Russian websites, as well as interrupting government and commercial websites and Internet connectivity in Georgia.

In 2008, the DoD got a wake-up call to the vulnerability of its computer systems when a foreign intelligence agent used a portable flash drive to infect computers at U.S. Central Command. The malware spread undetected across classified and unclassified computer systems in the most significant breach ever of DoD computers systems. DoD's Operation BUCKSHOT YANKEE countered the attack, which marked a turning point in U.S. cyber defense strategy. New security procedures were put in place, including banning of portable flash drives, and plans were made to centralize cyber defenses of military networks in a newly created DoD organization, U.S. Cyber Command (USCYBERCOM).

Defense Secretary Robert Gates ordered the creation of USCYBERCOM in June 2009 to assume the functions of Joint Task Force-Global Network Operations as a sub-unified command under U.S. Strategic Command. There also was a requirement for the services to create supporting cyber command elements by October 2010, when USCYBERCOM reached full operational capability.



In 2009, in an effort to delay Iran's development of a nuclear weapon, U.S. and Israeli intelligence agencies reportedly collaborated on a project called Operation OLYMPIC GAMES that successfully infected Iran's Natanz uranium enrichment facility computer systems with a virus called the Stuxnet worm that reprogrammed the centrifuges to fail. The virus may have been transmitted through a USB port memory drive. Stuxnet was the first computer virus to go after industrial systems and cause actual damage to a system. The spread of Stuxnet to systems in Indonesia and elsewhere subsequently led to its discovery in October 2010.

In January 2010, Spc. Bradley Manning, an Army intelligence analyst in Iraq (right), downloaded more than 450,000 documents, including classified State Department cables, pertaining to operations in Iraq and Afghanistan. The following month Manning provided the material to WikiLeaks, a website allowing whistleblowers to publicize sensitive material, which posted portions of the material online. Manning was arrested, demoted and sentenced to a 35-year prison term.

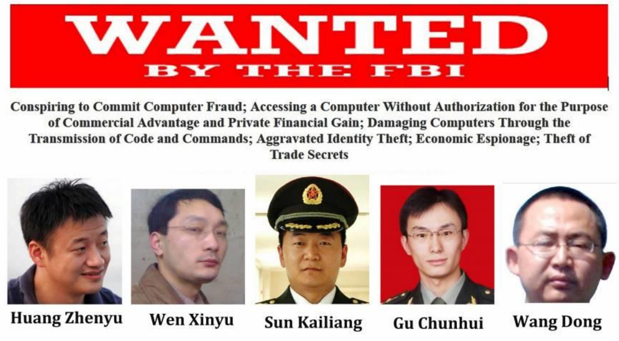
The Army established U.S. Army Cyber Command to support USCYBERCOM, on October 1, 2010, with its headquarters at Fort Belvoir, Va.

In March 2011, foreign hackers breached the DoD's computer system and stole 24,000 files, one of the largest breaches ever on DoD computers.

In 2013, Edward Snowden, an NSA contractor who grew increasingly concerned about government surveillance programs (right), leaked tens of thousands of classified NSA documents about these programs to the media. He justified his actions as a "whistleblower," and subsequently fled to Russia where he received temporary asylum.

In August 2013, the largest data breach to date occurred when state-sponsored hackers stole data from the Yahoo internet service company, including personal information, e-mail addresses, phone numbers and passwords, from more than a billion user accounts. The hackers forged "cookies" that allowed them to access accounts without a password. Yahoo did not became aware of the breach until December 2016.

In 2014, Russian hackers breached the State Department's unclassified computer system, which allowed them to then infiltrate the White House unclassified computer system. In October 2014, the White House and State Department uncovered the breaches, which included access to sensitive emails.



WANTED

BY THE FBI

Conspiring to Commit Computer Fraud; Accessing a Computer Without Authorization for the Purpose of Commercial Advantage and Private Financial Gain; Damaging Computers Through the Transmission of Code and Commands; Aggravated Identity Theft; Economic Espionage; Theft of Trade Secrets

Huang Zhenyu Wen Xinyu Sun Kailiang Gu Chunhui Wang Dong

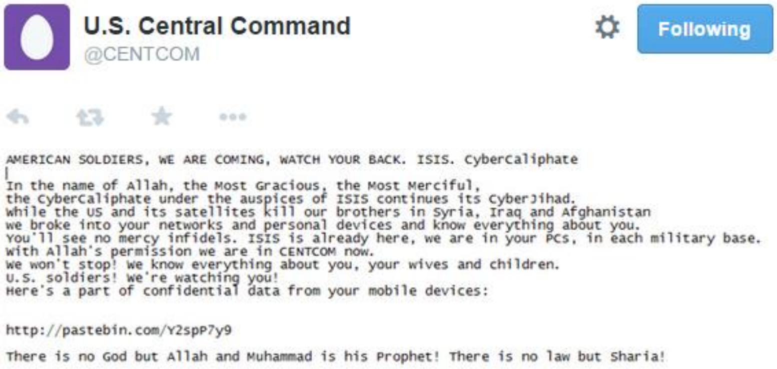
In May 2014, the U.S. indicted five Chinese People's Liberation Army officers for cyber economic espionage against six American commercial targets. The indictments marked the first charges against known state actors for cyber espionage.

In 2014, unknown hackers, believed to be Chinese, compromised the personal information of more than 20 million current and former federal employees in the Office of Personnel Management (OPM) computer network. The intrusions were discovered in 2015 during an OPM upgrade of its equipment and systems. Director of National Intelligence James R. Clapper noted that, "You have to kind of salute the Chinese for what they did" and went on to add, "The challenge here, the problem for us, frankly, is until such time as we can create both the substance and the psychology of deterrence, this is going to go on, and that's been frankly a struggle for us, because of concerns about unintended consequences and other related policy issues."

As the scope of private sector hacking increased, Iranian state-sponsored hackers stole data and erased hard drives belonging to the Las Vegas Sands Corporation, the world's largest gaming company, in February 2014. The attack came after Sands CEO Sheldon Adelson casually suggested that the U.S. drop a nuclear bomb on Iran. That year hackers also accessed about 83 million J.P. Morgan Chase bank accounts and compromised about 56 million Home Depot accounts. But the major hacking headline of the year occurred in November, when North Korean hackers attacked Sony Pictures Entertainment in retaliation for Sony's planned release of *The Interview*, a comedy about an assassination attempt on North Korean leader Kim Jong Un. The Sands and Sony hacks marked the first times foreign powers sought large-scale cyber retribution against U.S. corporations. In January 2015, after a North Korean official used racist language speaking about President Barack Obama and accused the U.S. of attacking his country's Internet, the president imposed increased sanctions against North Korea for the Sony hack.

In December, Congress passed the Federal Information Security Modernization Act of 2014, which revised and updated the earlier Federal Information Security Management Act and codified the Department of Homeland Security's role in administering implementation and oversight of information security policies for federal executive branch civilian agencies, and assisting the Office of Management and Budget in developing those policies.

That following month Islamic State Caliphate, or ISIS, hackers temporarily compromised U.S. Central Command's social media Twitter and YouTube accounts, putting out a string of tweets, such as the one depicted at right, as well as personal contact information for U.S. service members and threatening messages aimed at those waging war in Iraq and Syria.

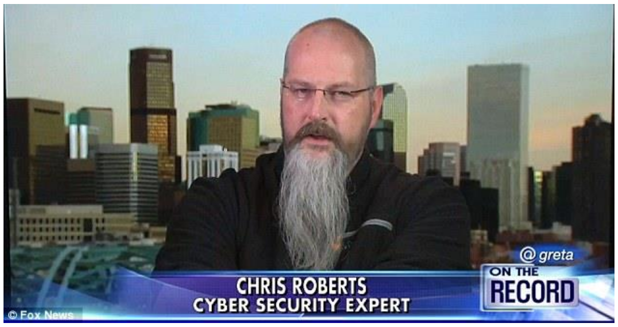


```
AMERICAN SOLDIERS, WE ARE COMING, WATCH YOUR BACK. ISIS. CyberCaliphate

In the name of Allah, the Most Gracious, the Most Merciful,
the CyberCaliphate under the auspices of ISIS continues its CyberJihad.
While the US and its satellites kill our brothers in Syria, Iraq and Afghanistan
we broke into your networks and personal devices and know everything about you.
You'll see no mercy infidels. ISIS is already here, we are in your PCs, in each military base.
With Allah's permission we are in CENTCOM now.
We won't stop! We know everything about you, your wives and children.
U.S. soldiers! We're watching you!
Here's a part of confidential data from your mobile devices:

http://pastebin.com/Y2spP7y9

There is no God but Allah and Muhammad is his Prophet! There is no law but Sharia!
```

In early 2015 Russian hackers infiltrated DoD's unclassified computer network. Director of National Intelligence Clapper told a Senate hearing the "Russian cyber threat is more severe than we have previously assessed."

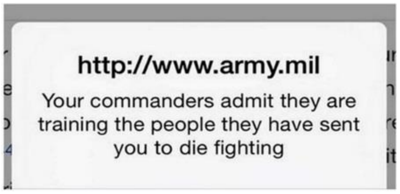
In a February attack on Anthem, one of the nation's largest health insurers, hackers suspected to be Chinese breached a database that contained as many as 80 million records of employees and current and former customers. The same month DoD researchers demonstrated remotely controlling a car with a laptop computer, a feat would be famously repeated later that year when two hackers remotely disabled a Jeep Cherokee via its "infotainment system."

A sophisticated hacker group, also thought to be Russian, nabbed personal information from more than 330,000 U.S. Internal Revenue Service accounts over several months in early 2015 and submitted fraudulent returns that cost the IRS about $50 million.



In April a Government Accountability Office report noted significant security weaknesses in U.S. air traffic control systems. Security researcher Chris Roberts (at left) was thrown off a United Airlines flight after claiming to have hacked into onboard systems via the aircraft's entertainment system. Roberts claimed to have hacked into more than a dozen previous flights and had conferred with the FBI and aircraft manufacturers about his findings.

In June 2015 a group calling itself the Syrian Electronic Army compromised the U.S. Army's official public website demanding the U.S. stop training rebel fighters in Syria. The Army temporarily took down the site after the hackers posted messages such as the one depicted at right.



http://www.army.mil

Your commanders admit they are training the people they have sent you to die fighting

The following month Russian hackers breached the Joint Chiefs of Staff unclassified email server via a spear-phishing attack – a tactic used to trick people into opening infected emails that steal their network credentials and spread through a network. The attack affected about 4,000 users and caused the email network to be taken offline for more than 10 days.

That same month the FBI, working with international law enforcement agencies, closed a major malware marketplace called Darkode, which had been operating since at least 2008. The crackdown resulted arrests in 20 countries and 70 indictments, including 12 in the U.S.

An advanced group linked to Russian military intelligence reportedly launched the first major cyber attack against a nation's air traffic control system in early November. The cyber attack, which grounded hundreds of flights in Sweden and was publicly attributed to solar flares, focused on radar systems that made computer screens go blank.

Belarus
Russia
Poland
Kyiv
Kharkov
Slovakia
Ukraine
Donetsk
Dnepropetrovsk
Moldova
Dnieper
Sea of Azov
Odessa
Romania
Black Sea

In December 2015 hackers reportedly working for Russia shut down a substantial part of Ukraine's electrical grid, marking a significant cyber attack against a national infrastructure.

The DoD announced U.S. Cyber Command's first wartime mission – disrupting Islamic State (ISIL) computer networks in Iraq and Syria – in February 2016. In May, USCYBERCOM created Joint Task Force Ares, headed by Lt. Gen. Edward C. Cardon, commander of U.S. Army Cyber Command, to execute the counter-ISIL mission.

The following month North Korean hackers breached the smartphones of some top South Korean government officials. The North Korean military hacking unit, known as Bureau 121, reportedly included approximately 6,000 trained hackers. In September North Korean hackers also reportedly breached the South Korean army cyber command and gained access to confidential material.

The U.S. government ran its first bug bounty program, called "Hack the Pentagon," from April to May 2016, to identify and resolve security vulnerabilities in five DoD public-facing websites. More than 1,400 participants were given legal consent for specific hacking techniques. The program was very successful, with the first vulnerabilities reported 13 minutes after it began.

In June 2016 LinkedIn said it was investigating a user's post from a Russian forum that claimed the user had hacked the business networking site. The post had included more than 6 million encrypted passwords as proof. More than 100 million users' passwords were leaked, as well as user IDs and email addresses.

The same month the Democratic National Committee discovered that two cyberespionage groups linked to Russian military intelligence, had breached its computer systems for about a year. The hackers leaking documents in what was believe to be an attempt to undermine Hillary Clinton's bid for the U.S. presidency. In October, for the first time, the U.S. government accused Russia of state-sponsored hacking and sanctioning the theft and leaking of more than 19,000 DNC emails. The Russian government denied complicity in the attacks and attempts to influence the election.

On October 21, major websites across the internet in Europe and North America were inaccessible for about 11 hours due to a series of distributed denial of service attacks against the Dyn corporation. Using malware to take over online devices such as cameras, baby monitors and home routers, hackers overwhelmed their target with traffic from tens of millions of internet addresses. The groups Anonymous and World Hackers claimed responsibility for the attacks.

In mid-December Yahoo announced that a breach of its systems, in which hackers used forged cookies to enter 500 million user accounts without a password and steal data, including personal information, e-mail addresses, phone numbers and passwords. The breach, traced back to 2014, ultimately affected 1 billion of its users. Yahoo blamed a "state-sponsored actor" for the attack, but did not identify its suspect.

Criminal hackers breached San Francisco's municipal transportation system in November, using ransomware to lock files behind an encrypted paywall and disable ticket kiosks. Although they gained access to about 25 percent of the transportation authority's office computers, they did not breach its operational network, and their demand for a ransom of 100 Bitcoin ($73,000) was not paid.

As 2016 ended, President Obama announced December 30 that the U.S. was expelling 35 Russian diplomats, shutting down two U.S. facilities authorities said were used for Russian intelligence activity, and penalizing four top officers of Russia's GRU intelligence service, in response to Russian "cyber-meddling" in the U.S. presidential election. Russian president Vladimir Putin rejected calls for retaliation against the U.S., suggesting that he would pursue normalizing relations through discussions with the Trump administration.